UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,446	07/31/2003	Amit Raikar	200300489-1	2839

22879 7590 06/13/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

NOTIFICATION DATE	DELIVERY MODE
06/13/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/632,446
Filing Date: July 31, 2003
Appellant(s): RAIKAR ET AL.

John P. Wagner, Jr.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 3/17/08 appealing from the Office action mailed 11/16/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20030188189	**Desai et al.**	3-2002
6,957,348	**Flowers et al.**	1-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-19 are presented for examination. These rejections are set forth in prior Office Action, Paper No. 10/632,446\20071030 and reproduced for convenience.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claim **1 - 7, 14 - 19** are rejected under 35 U.S.C. 102(e) as being anticipated by **Desai et al.** (US PGPUB No. **20030188189**).

Regarding Claim 1, Desai discloses a method for configuring templates, the method comprising:

a) configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked)

b) configuring the template with second information for processing the data associated with at least one of the received messages; (see Desai paragraph [0093], lines 3-6: processing data, execute user defined programs) and

c) configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system. (see Desai paragraph [0063], lines 1-4: further analysis)

Regarding Claims 2, 15, Desai discloses the method, computer system of claims 1, 14, wherein configuring the template with second information for processing further comprises configuring the template with the second information for communicating the data associated with at least one of the received messages to a management server. (see Desai paragraph [0063], lines 1-4: forwarded to management server)

Regarding Claims 3, 16, Desai discloses the method, computer system of claims 1, 14, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template. (see Desai paragraph [0043], lines 3-8; paragraph [0090], lines 4-10: SNMP, or logfile processing)

Regarding Claims 4, 17, Desai discloses the method, computer system of claims 1, 14, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources. (see Desai paragraph [0050], lines 1-4; paragraph [0052], lines 1-6: matching utilized for analysis)

Regarding Claims 5, 18, Desai discloses the method, computer system of claims 1, 14, wherein the method further comprises: configuring the template with fourth information for specifying for a particular received message an action to be performed, wherein the fourth information ensures that the action is performed on a node that generated the particular received message. (see Desai paragraph [0058], lines 4-6; paragraph [0061], lines 7-11: event threshold parameter assigned to specific originating device)

Regarding Claims 6, 19, Desai discloses the method, computer system of claims 1, 14, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:

a) configuring the template with the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked) and

b) configuring the template with the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates. (see Desai paragraph [0063], lines 1-4: further analysis)

Regarding Claim 7, Desai discloses the method of claim 1, wherein the steps of configuring are performed by a template automator. (see Desai paragraph [0024], lines 1-3; paragraph [0062], lines 3-6; paragraph [0089], lines 5-9: automatic processing)

Regarding Claim 14, Desai discloses a computer system comprising:

a) a memory unit; (see Desai paragraph [0012], lines 10-12: web server, network server, workstation) and

b) a processor coupled to the memory unit (see Desai paragraph [0012], lines 10-12: web server, network server, workstation), wherein the processor executes instructions associated with a template automator, and wherein the instructions of the template automator are for:

c) configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked)

d) configuring the template with second information for processing the data associated with at least one of the received messages; (see Desai paragraph [0093], lines 3-6: processing data, execute user defined programs) and

e) configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system. (see Desai paragraph [0063], lines 1-4: further analysis)

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim **8 - 13** are rejected under 35 U.S.C. 103(a) as being anticipated by **Desai et al.** (US PGPUB No. **20030188189**) in view of **Flowers et al.** (US Patent No. **6,957,348**).

Regarding Claim 8, Desai discloses a method for providing a guideline to developers for creating templates, the guideline comprising information used by the developers for:

a) receiving first information entered by a developer to configure a template of an application and network management system for determining whether data associated with at least one message received by the template should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked)

b) receiving second information entered by the developer to configure the template to process the data associated with at least one of the received messages; (see Desai paragraph [0093], lines 3-6: processing data, execute user defined programs) and

c) receiving third information entered by the developer to configure the template to prevent the communication of at least one received message to other templates of the application and network management system. (see Desai paragraph [0063], lines 1-4: further analysis)

Desai does not specifically disclose the guidelines for developers. However, Flowers discloses wherein providing a guideline to developers for creating

templates, the guideline comprising information used by the developers. (see Flowers col. 2, lines 45-50; col. 2, lines 53-60: development of templates, rules)

It would have been obvious to one of ordinary skill in the art to modify Desai as taught by Flowers to enable the capability to provide a guideline comprising information used by the developers for creating templates. One of ordinary skill in the art would have been motivated to employ the teachings of Flowers in order to enable the capability to enable the identification and description of vulnerability and intrusion detection information for typical network engineers in development efforts. (see Flowers col. 2, lines 16-18: *" ... Further, there is a need to perform vulnerability and intrusion identification and description that is usable by typical network engineers. ... "*)

Regarding Claim 9, Desai discloses the method of claim 8, wherein configuring the template with second information for processing further comprises configuring the template with the second information for communicating the data associated with at least one of the received messages to a management server. (see Desai paragraph [0063], lines 1-4: forwarded to management server)

Regarding Claim 10, Desai discloses the method, of claim 8, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template. (see Desai paragraph [0043], lines 3-8; paragraph [0090], lines 4-10: SNMP, or logfile processing)

Regarding Claim 11, Desai discloses the method of claim 8, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources. (see Desai paragraph [0050], lines 1-4; paragraph [0052], lines 1-6: matching utilized for analysis)

Regarding Claim 12, Desai discloses the method of claim 8, wherein the method further comprises: configuring the template with fourth information for specifying for a particular received message an action to be performed, wherein the fourth information ensures that the action is performed on a node that generated the particular received message. (see Desai paragraph [0058], lines 4-6; paragraph [0061], lines 7-11: event threshold parameter assigned to specific originating device)

Regarding Claim 13, Desai discloses the method of claim 8, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:

a) configuring the template with the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked) and

b) configuring the template with the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates. (see Desai paragraph [0063], lines 1-4: further analysis)

(10) Response to Arguments

1. Claims **1 - 7** and **14 - 19** are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication no. 20030188189 by Desai et al. (referred to herein as "Desai").

2. Claims **8 - 13** are rejected under 35 U.S.C. §103(a) as being unpatentable over Desai in view of U.S. Patent No. 6,957,348 by Flowers et al. (referred to herein as "Flowers").

A.1 Desai does not disclose "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template". (Appeal Page 12)

Response:

Applicant has repeatedly stated within Appeal Remarks the logfile data processing aspect of Desai. Desai processes data from all sources real-time and near real-time sources (logfile data). In fact, the specification discloses that logfile data is processed in

the claimed invention. (Specification page 11, ll 2-6; page 11, ll 18-21: system logfile information processed by template information)

There is nothing in the specification or the original claims that discourages, discredits, or "teaches away" from the usage of logfile information in the processing of an event message and its associated data using the template data structure dictating how to process event messages.

There is nothing in the claimed invention indicates that logfile data is not to be processed and there is no indication that real-time data is the only data to be processed. In addition, Claim 10 discloses a logfile template is used to process event messages. It is unclear why a question of whether Desai processes all of its log files has any bearing on the prior art. (Appeal Remarks Page 17) Desai discloses that not every event message is processed. (Desai para 055, lines 1-14: selective information is processed; increasing or decreasing logging information for different types of services (event processing) and other types of traffic) The logfile contains a plurality of selective event messages.

Applicant's invention discloses configuring a template. Desai discloses configuring a template. There is no disclosure of any real-time configuration of a template. The templates in question are used to process event messages.

Desai discloses that real-time information in addition to near real-time information such as within a logfile is processed. (Desai para 037, ll 1-6: real-time response capabilities; para 083, ll 1-6: event correlation unit enables real-time and historical views

of events processed; para 043, ll 3-8: log are sent in real-time through secure channel to secure log/event collector) The template data structure and associated data is used to determine whether a particular event message is to be processed or not.

Desai discloses a determination to process event messages concerning a particular event or not to process the event messages.

If a session has been terminated then all event messages associated with that particular session are of no use to the Intrusion Detection System (real-time or near real-time data) and would not need to be processed. Session information would be data associated with an event message and is eligible for processing by the template. Based on the session termination status, the event messages would not need to be processed. (Desai para 089, ll 7-11: particular session terminated)

A.2 Desai does not disclose "configuring the template with second information for processing the data associated with at least one of the received messages". (Appeal Page 12)

Response:

Desai discloses processing an event message and associated data based on the template. This is the "normal" type of processing for analysis and correlation of event messages and their associated data. (Desai para 049, ll 1-7: event messages are processed through an event analysis engine; para 053, ll 1-7: applies filtering techniques) Desai discloses real-time and near real-time processing of an event

message and its associated data. The network management event messages indicate that some network related event has occurred and the event analysis engine determines whether any further actions are required to protect the network.

A.3 Desai does not disclose "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system". (Appeal Page 12)

Response:

Desai discloses a determination to process event messages concerning a particular event or not to process the event messages.

If no further processing and analysis is required for event message pertaining to a particular session, the event message and associated data are not processed further or no additional filtering is completed. The session has been terminated. There is no disclosure that all event messages are processed based on the fact that logfile data is processed. Desai also disclose that real-time data is processed.

A.4 Desai teaches away from "determining whether data should not be processed". (Appeal Page 13)

Response:

There is no disclosure in Desai to discourage or discredit the capability to determine whether data should not be processed. There is no disclosure in Desai that all data

encountered is processed. Applicant seems to based his assertion that all data is processed (Appeal Remarks Page 17) or the fact that Desai mentions logfile type data as one type of information processed.

Applicant has repeatedly mentioned logfile type data is processed by Desai. There is no requirement that real-time or non-real-time data must be processed or not processed by the claimed invention or even mentioned in the specification. Desai disclose that not all data is processed as logfile data. (Desai para 055, lines 1-14: selective information is processed; increasing or decreasing logging information for different types of services (event processing) and other types of traffic)

Desai discloses that in the event a session is determined to be abnormal, that particular session is terminated. In this situation, event messages pertaining to that particular session need not be processed. There is no need to process and correlate event data for this session to determine whether the session is abnormal. That determination has already been made. This satisfies the requirement of a determination to not process an event message based on the associated data such as session information.

Desai does disclose additional features not available in the claimed invention. Since these additional do not teach away from the claimed invention, these additional features do not impact the prior art's ability to disclose applicant's claimed invention.

Conclusion

Desai discloses the processing of event type messages using template data structures, which determine how to process the event messages. Desai discloses the processing of all types of event messages in real-time and near real-time environments. Desai discloses that not all event messages that occur are processed. The set of event messages eligible for processing are reviewed and adjusted at regular intervals. Desai disclose the ability to determine what to process and what not to process.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
June 8, 2008

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2154

Conferees:

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2154

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151